REMARKS

Claims 37 and 53 have been canceled. Claims 1, 18, 35, 36 and 38 have been amended. Claims 1-36, 38-52 and 54 are pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 112, First Paragraph, Rejection:

The Examiner rejected claims 1-36, 38-52 and 54 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. In regard to claims 1-35, 38-52 and 54 the Examiner asserts, "[t]he specification fails to mention or teach the limitation wherein transmitting a response to a remote authorization unit to authenticate a response without transmitting the passcode to the remote authorization unit and without generating the passcode from the user input prior to said transmitting." (Office Action, November 12, 2009, pp. 2-3). In regard to claim 36, the Examiner asserts, "[t]he specification fails to mention or teach the limitation wherein validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code." (Office Action, November 12, 2009, p. 3). Applicant respectfully traverses these rejections.

Applicant respectfully directs the Examiner to pg. 10, lines 6-13 of Applicant's specification, which reads (emphasis added):

> the user response may be transmitted to some remote unit, such as a security system, to authenticate the entered response. Note that the **entered pass code per se might never be calculated**. For example, the security system might predict the response to be entered by a user, based on knowledge of the challenge and the authentic pass code. The response received from the user can then be tested against this prediction, and if there is a match, the response from the user corresponds to what was expected, and so the user is validated.

In regard to claims 1-35, 38-52 and 54, this passage of Applicant's specification clearly describes an example where the user response is transmitted to a remote unit for authentication without calculating the pass code per se. Accordingly, Applicant's

specification explicitly supports the recitation in the claim of transmitting ... without generating the pass code from the user input prior to said transmitting. Moreover, if the pass code is not generated, then the user response transmitted to the remote unit clearly cannot be the pass code. Thus, the specification also supports transmitting ... without transmitting the pass code to the remote authorization unit. Furthermore, Applicant's specification clearly distinguishes the user response from the pass code. For example, Applicant's specification states, "[t]he method involves providing a user with a machine-generated challenge, and receiving a **response from the user**. The **response** represents a **transformation from the challenge** provided to the user **to a pass code** allocated to the user." (Specification, p. 8, lines 14-16). It is clear from the specification that the transmitted user response is not the pass code and cannot be the pass code, since the response is a transformation and the pass code might never generated prior to transmitting the response. Applicant asserts that the claim language "without transmitting the passcode to the remote authorization unit and without generating the passcode from the user input prior to said transmitting" is clearly supported by Applicant's specification. Accordingly, Applicant respectfully requests removal of the under 35 U.S.C. § 112, first paragraph rejection of claims 1-35, 38-52 and 54.

In regard to claim 36, the above-cited passage from pg. 10 of Applicant's specification describes testing the user response against a predicted response based on knowledge of the challenge and the authentic pass code. As described above, Applicant's specification explicitly describes an example where **the pass code is not calculated**. Accordingly, neither the user response nor the predicted response can be the pass code, since the pass code is not calculated. Furthermore, as described above, Applicant's specification distinguishes the user response from the pass code. Applicant's specification also clearly distinguishes the predicted response from the pass code. Applicant's specification clearly describes that neither the user response nor the predicted response is the pass code. Therefore, Applicant asserts that the claim language "validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code," is supported by

Applicant's specification. Accordingly, Applicant respectfully requests removal of the under 35 U.S.C. § 112, first paragraph rejection of claim 36.

As repeatedly stated by the Board of Patent Appeals & Interferences and by the Court of Appeals for the Federal Circuit, **it is well settled that the claimed invention does not have to be described in *ipsis verbis* in order to satisfy the description requirement of §112**. *Jacobs v. Lawson*, 214 USPQ 907, 910 (B.P.A.I. 1982) (emphasis added). "The subject matter of the claim **need not be described literally** in order for the disclosure to satisfy the description requirement." *M.P.E.P. 2163.02* (emphasis added). As longs as the description "allows persons of ordinary skill in the art to recognize that [the inventors] invented what is claimed" then the description requirement is satisfied. *In re Gosteli*, 10 USPQ2d 1614, 1618 (Fed. Cir. 1989). As shown above, when Applicants' specification is considered as a whole, one skilled in the art would easily recognize the claimed invention. The Examiner's application of the description requirement in the Final Action is "yet another instance of the sort of 'hypertechnical application' of the written description requirement of §112" that has been repeatedly criticized by the court. *In re Driscoll*, 195 USPQ 434, 438 (C.C.P.A. 1977); *In re Johnson*, 558 F.2d 1008, 194 USPQ 187 (CCPA 1977); *Engineering Development Laboratories v. Radio Corp. of America*, 68 USPQ 238, 241-42 (2d Cir. 1946).

Furthermore, the Board has held that "a bare assertion by the Examiner" is insufficient for an assertion that the description requirement is not met. *Ex parte Sorenson*, 3 USPQ2d 1462, 1463 (Bd. Pat. App. & Inter. 1987). The Examiner has the burden to present evidence or reasons, not just bare assertions, why persons skilled in the art would not recognize support for the claimed invention. *In re Wertheim*, 191 USPQ 90 (CCPA 1976). In the rejection the Examiner did nothing more than make a "bare assertion" that certain limitations were not supported. The Examiner did not provide any evidence or reasons. Therefore, the rejection is improper.

Section 112, Second Paragraph, Rejection:

The Examiner rejected claims 1-36, 38-52 and 54 under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. The Examiner asserts "[i]n claims 1, 18, 35, 36 and 38 the phrase 'capable of' renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention." (Office Action, November 12, 2009, pp 2-3). Claims 1, 18, 35, 36 and 38 have been amended in response to the Examiner's comments. Applicant asserts these claim amendments clarify the claim language. Accordingly, Applicant respectfully requests withdrawal of the §112, second paragraph, rejection for claims 1-36, 38-52 and 54.

Section 103(a) Rejections:

The Examiner rejected claims 1-16, 18-33 and 35-53 under 35 U.S.C. § 103(a) as being unpatentable over Hoover (U.S. Patent 5,721,779) in view of Weiss (U.S. Patent 5,023,908), and claims 17, 34 and 54 as being unpatentable over Hoover in view of Weiss, and further in view of Funk (U.S. Patent 5,721,779). Applicant respectfully traverses these rejections for at least the following reasons.

In regard to claim 1, the cited art fails to teach or suggest *generating a response from the user input received from the user input device, wherein the* ***user input does not include the pass code itself*** *and transmitting the response to a remote authorisation unit to authenticate the response* ***... without generating the pass code from the user input prior to said transmitting***. The Examiner admits that Hoover does not teach this limitation and relies on Weiss to teach it, citing Weiss col. 3, line 45 – col. 4, line 28. Weiss at col. 4, lines 15 – 33 recites, in pertinent part:

> the user is **inputting his PIN** into his device.... The next step in the operation, step 38, is for the g**enerated nonpredictable code and the inputted pin to be mixed** by the processor in device 10 to generate a new nonpredictable code which is displayed on display 14. (emphasis added)

Weiss clearly discloses that a user's PIN is **included** in the user's input. Furthermore, Weiss discloses that the user **input PIN** is mixed with a nonpredictable code. In contrast,

Applicant's claim requires that the pass code is neither included in the user input nor generated prior to transmitting a response. Weiss receives a user PIN **included** in user input and uses the PIN to generate a nonpredictable code. Accordingly, Applicant asserts that neither Weiss, nor any of the other cited references, whether considered alone or in combination, teach or suggest *generating a response from the user input received from the user input device, wherein the* ***user input does not include the pass code itself*** *and transmitting the response to a remote authorisation unit to authenticate the response* ***... without generating the pass code from the user input prior to said transmitting***.

Further in regard to claim 1, the cited art fails to teach or suggest *transmitting the response to a remote authorisation unit ... wherein said response allows the user to be validated at the remote authorisation unit dependent on* ***said response compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code***. The Examiner relies on Weiss to teach this limitation, citing col. 3, line 45 – col. 4, line 28 of Weiss. The cited passage of Weiss recites in pertinent part:

> the user may input his unique PIN on areas 12 which are mixed in the processor in device 10 with the **nonpredictable code generated therein in response to the time-dependent and static inputs** to generate a multi-bit nonpredictable code .... In response to the user input of his nonsecret code, the verification computer retrieves the user's PIN and **generates the nonpredictable code** for the user, **using the same algorithm and stored static value as user device 10, and using a time-related value from a clock device at the verification computer, which is maintained in synchronism with the clock at the user device** in a manner discussed in the parent application (step 32). ... While the user is inputting his pin, the user device is continuously generating **nonpredictable code values at its internal processor in response to the clock value and the stored static value using the unique algorithm at the user device processor**. (emphasis added)

Weiss does not teach a **predicted** response. In contrast, Weiss discloses a **nonpredictable** code generated in response to time-dependent and static inputs, as described in the above-cited passage. The Examiner has apparently misinterpreted the reference, as in the Examiner's cited passage, Weiss explicitly describes a

nonpredictable code. A **nonpredictable** code is clearly not the same as a **predicted** response. Moreover, not only is Weiss' nonpredictable code not a predicted response, Weiss' nonpredictable code is not based on **knowledge of a challenge** and a stored data record of the pass code, as required by Applicant's claim 1. Weiss describes, "[t]he device 10 has a clock which generates a time dependent digital output to a microprocessor which is programmed with a unique algorithm to operate on the **time-dependent clock input** and on a stored static value unique to a given user to generate a multi bit **nonpredictable** code." (Weiss, col. 3, lines 31-36). (emphasis added) In other words, Weiss explicitly describes that the nonpredictable code is based on a **time-dependent clock input** and a stored static value. A time-dependent clock input is not the same as knowledge of a challenge. Weiss makes absolutely no mention of a machine-generated challenge. Clearly, the nonpredictable code of Weiss is not based on knowledge of a machine-generated challenge and cannot be based on a machine-generated challenge since Weiss makes no mention of such a challenge.

Furthermore, Weiss does not describe validating a user dependent on a **user input response compared to a predicted response** based on knowledge of a challenge and a stored data record of a pass code. Weiss describes, "the verification computer uses the PIN for the user which was retrieved during step 32 to strip the PIN from the inputted nonpredictable code, the result being a PIN value and a nonpredictable code value. During step 44 the **stripped PIN is compared with the PIN retrieved** during step 32 and during step 46 **the nonpredictable code remaining after the inputted value has the PIN stripped therefrom is compared with the retrieved nonpredictable code**. If matches are obtained during both steps 44 and 46 (step 48) the verification computer signifies verification." (Weiss, col. 4, lines 34-45). (emphasis added) In other words, to verify a user, Weiss describes comparing a transmitted PIN to a retrieved PIN and comparing a transmitted nonpredictable code to a retrieved nonpredictable code. None of these values used by Weiss for validating a user are a **predicted response** based on knowledge of a challenge and a stored data record of a pass code. Accordingly, Weiss does not validate a user dependent on a **user input response compared to a predicted response**. Weiss explicitly describes validating a user by comparing **PIN values** and

nonpredictable codes. Hoover does not overcome the above-noted deficiencies of Weiss. Applicant asserts that no combination of the cited art teaches or suggests *transmitting the response to a remote authorisation unit ... wherein said response allows the user to be validated at the remote authorisation unit dependent on* ***said response compared to a predicted response*** *based on* ***knowledge of the challenge and a stored data record of the pass code***.

Furthermore, the Examiner has not stated a proper reason to combine the teachings of the cited art. The Examiner asserts that it would have been obvious to combine the teachings of Weiss with the teachings of Hoover "in order to enhance the security of the system." (Office Action, November 12, 2009). However, there is no evidence that this reason would be achieved by the combination suggested by the Examiner, as Hoover already contains a method for enhancing security. Hoover's system enhances security by "protecting a user's PIN, password, or other access code, from disclosure to an attacker." (Hoover, col. 1, lines 57-58). The Examiner has provided no evidence that the teachings of Weiss would enhance the security measures disclosed by Hoover to protect a user's PIN. As stated in *KSR Int'l Co. v. Teleflex Inc.*, No. 04-1350, slip. op. at 14 (U.S. Apr. 30, 2007), "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal standard of obviousness." The Examiner must show that "there was an apparent reason to combine the known elements in the fashion claimed." *Id.* The Examiner's analysis "should be made explicit." *Id.* Mere conclusory statements are insufficient. The Examiner's stated reason to combine the reference lacks a rational underpinning since Hoover already achieves the purpose stated by the Examiner as an obvious reason to combine. Moreover, as shown above, the proposed combination would not result in Applicant's claimed invention, as both Hoover and Weiss explicitly disclose generating and transmitting a pass code and neither generates a predicted response based on knowledge of a challenge and a stored data record of the pass code. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

For at least the reasons above, the rejection of claim 1 is unsupported by the cited art and removal thereof is respectfully requested.

Independent claims 18 and 38 recite limitations similar to those discussed above regarding claim 1, and were rejected using similar reasoning. Therefore, the arguments presented above apply similarly to these claims.

In regard to claim 35, the cited art fails to teach or suggest *means for generating a response from the user input received from the user input device, wherein the* ***user input does not include the pass code itself*** *and means for transmitting the response to a remote authorisation unit to authenticate the response* ***... without generating the pass code from the user input prior to said transmitting***. The Examiner admits that Hoover does not teach this limitation and relies on Weiss to teach it, citing Weiss col. 3, line 45 – col. 4, line 28. As described above in regard to claim 1, Weiss clearly discloses that a user's PIN is **included** in the user's input. Furthermore, Weiss discloses that the user **input PIN is mixed** with a nonpredictable code. In contrast, Applicant's claim requires that the pass code is neither included in the user input nor generated prior to transmitting a response. Weiss receives a user PIN **included** in user input and uses the PIN to generate a nonpredictable code. Accordingly, Applicant asserts that neither Weiss, nor any of the other cited references, whether considered alone or in combination, teach or suggest *means for generating a response from the user input received from the user input device, wherein the* ***user input does not include the pass code itself*** *and means for transmitting the response to a remote authorisation unit to authenticate the response* ***... without generating the pass code from the user input prior to said transmitting***.

For at least the reasons above, the rejection of claim 35 is unsupported by the cited art and removal thereof is respectfully requested.

In regard to claim 36, the cited art fails to teach or suggest *generating a* ***predicted*** *response based on knowledge of the challenge and a stored version of the pass code and* ***validating the user on the basis of said response compared to the predicted response,***

wherein ***neither the response nor the predicted response is the pass code.*** Applicant notes that the Examiner **fails to provide any remarks** directed to a user input response and a predicted response, wherein **neither the user input response nor the predicted response is a pass code**. Thus, a *prima facie* rejection has not been stated. Neither Hoover nor Weiss disclose a **predicted** response, much less a **predicted** response that is not a pass code. Furthermore, as described above in regard to claim 1, the cited art, whether considered alone or in combination, does not teach or suggest generating a **predicted response** based on knowledge of the challenge and a stored version of the pass code and **validating the user on the basis of said response compared to the predicted response**. In contrast, Weiss explicitly discloses a **nonpredictable** code generated in response to a time-dependent clock input and a static value. Weiss' nonpredictable code is not the same as a predicted response, and, furthermore, Weiss' nonpredictable code is not based on knowledge of a challenge and a stored data record of a pass code, as required by Applicant's claim 36. Furthermore, as described above in regard to claim 1, Weiss explicitly describes validating a user by comparing **PIN values** and **nonpredictable codes**, not dependent on a **user input response compared to a predicted response** based on knowledge of a challenge and a stored data record of a pass code, as required by Applicant's claim 36. Applicant asserts that none of the cited art, whether considered alone or in combination, teaches or suggests *generating a* ***predicted*** *response based on knowledge of the challenge and a stored version of the pass code and* ***validating the user on the basis of said response compared to the predicted response,*** *wherein* ***neither the response nor the predicted response is the pass code.***

For at least the reasons above, the rejection of claim 36 is unsupported by the cited art and removal thereof is respectfully requested.

In regard to claim 17, contrary to the Examiner's assertion, the cited art clearly fails to teach or suggest *using the response to encrypt said communications challenge and transmitting the encrypted communications challenge to the authorisation unit; thereby allowing the response to be validated by said authorisation unit using said stored data record of the pass code.* On p. 8 of the Office Action dated November 12, 2009, the

Examiner admits Hoover fails to teach using the response to encrypt the communications challenge and relies on Funk, citing column 4, lines 50-52. Funk is directed to utilizing a challenge and response handshake to allow a server to authenticate a client based on a password. Column 4, lines 50-53 of Funk state: "The client can generate this response signal by employing the same one-way commutative function to encrypt the challenge signal, C, with one valid password." Funk uses the actual password to generate the response. Column 4, line 59 of Funk provides the following formula: Response=$F(C,$ Password)=$C^{password}$ mod q. In contrast, Applicant's claim 17 requires using the user response (i.e., transformation of the challenge), **not the actual pass code**, to encrypt the communications challenge. Both Hoover and Funk use the **actual** PIN or password in their respective designs. Neither reference, whether considered alone or in combination, teaches or suggests using the response (that is not the PIN/password) to encrypt the communications challenge and transmit the encrypted communications challenge to the authorisation unit. Thus, Funk combined with Hoover would not result in Applicant's claimed invention. Accordingly, the Examiner has failed to establish a *prima facie* case of obviousness.

For at least the reasons above, the rejection of claim 17 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 34 and 54 recite limitations similar to those discussed above regarding claim 17, and were rejected using similar reasoning. Therefore, the arguments presented above apply similarly to these claims.

Applicant also asserts that numerous other ones of the dependent claims recite further distinctions over the cited art. Applicant respectfully traverses the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time. Applicant reserves the right to present additional arguments.

CONCLUSION

Applicant submits the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5681-74900/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicant

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: February 12, 2010